Claims

1. An encrypting apparatus encrypting first processing data and second processing data comprising:

a memory for storing status of encrypting process, and

wherein the encrypting apparatus starts encrypting process of the second processing data before encrypting process of the first processing data is completed,

the encrypting apparatus makes the memory store the status of encrypting process of the first processing data when the encrypting apparatus starts encrypting process of the second processing data,

the encrypting apparatus returns the status of the encrypting process of the encrypting apparatus to the status of the encrypting process of the first processing data stored in the memory when the encrypting apparatus restarts encrypting the first processing data, and

the encrypting apparatus restarts encrypting process of the first processing data.

2. The encrypting apparatus of claim 1, wherein the encrypting apparatus restarts encrypting process of the first processing data before encrypting process of the second processing data is completed,

the memory stores the status of encrypting process of the second processing data when the encrypting apparatus restarts encrypting process of the first processing data,

the encrypting apparatus returns the status of the encrypting process of the encrypting apparatus to the status of the encrypting process of the second processing data stored in the memory when the encrypting

apparatus restarts encrypting process of the second processing data, and

the encrypting apparatus restarts encrypting process of the second processing data.

3. The encrypting apparatus of claim 1, wherein the first processing data is first plaintext data and the second processing data is second plaintext data.

4. The encrypting apparatus of claim 1, the encrypting apparatus starts encrypting process of the second processing data by an interrupt.

5. An encrypting apparatus encrypting plaintext data M including plaintext block data M_i (i = 1, 2, 3, ...) and plaintext data N including plaintext block data N_j (j = 1, 2, 3, ...), the encrypting apparatus comprising:

a mechanism for receiving a request to encrypt the plaintext data N during encrypting process of the plaintext data M;

an encrypting unit for encrypting the plaintext block data M_i to output ciphertext block data C_i;

a feedback loop for feeding back the ciphertext block data C_i output from the encrypting unit to the encrypting unit through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving a request to encrypt the plaintext data N and stores the ciphertext block data C_i fed back when the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i so that the encryption process of any of the plaintext block data of the plaintext data N is started; and

a selector for selecting and supplying the ciphertext block data C_i fed back from the feedback line of the feedback loop to the feedback loop in case

that the plaintext block data M_{i+1} is encrypted subsequent to the plaintext block data M_i, and for selecting and supplying the ciphertext block data C_i stored in the memory to the feedback loop in case that the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i and the plaintext block data M_{i+1} is encrypted after any of the plaintext block data of the plaintext data N is encrypted.

6. The encrypting apparatus of claim 5, wherein the memory includes:

plural registers corresponding to plural pieces of plaintext data; and

a switch for switching the plural registers corresponding to the plaintext data to be encrypted.

7. An encrypting method comprising the steps of:

encrypting plaintext block data M_i (i = 1, 2, 3, ...) of first plaintext data M using ciphertext block data C_i (i = 1, 2, 3, ...) output from an encrypting module;

storing ciphertext block data C_i to be used for encrypting plaintext block data M_{i+1} of the first plaintext data M in a memory during or after encrypting process of the plaintext block data M_i;

encrypting at least one plaintext block data of second plaintext data N after storing the ciphertext block data C_i to be used for encrypting the plaintext block data M_{i+1} in the memory; and

encrypting the plaintext block data M_{i+1} of the first plaintext data M by inputting the ciphertext block data C_i to be used for the plaintext block data M_{i+1} stored in the memory and using the encrypting module after encrypting the at least one plaintext block data of the second plaintext data N.

8. An encrypting apparatus encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the encrypting apparatus comprising:

an encrypting unit, having a first feedback loop for feeding back ciphertext block data C_i output by the encrypting unit to the encrypting unit when the plaintext block data is encrypted by the encrypting unit, for inputting the plaintext data, performing an encrypting process by feeding back the ciphertext block data C_i through the first feedback loop, and outputting the ciphertext block data;

a message authentication code (MAC) generator, having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting unit, processing data, feeding back the computed intermediate MAC result by the second feedback loop, and generating the MAC to ensure the integrity of the ciphertext data.

9. The encrypting apparatus of claim 8,

wherein the encrypting unit and the MAC generator perform alternately the encrypting process and a MAC generating process by sharing one encrypting module and one feedback loop, and

wherein the one feedback loop includes:

a memory for respectively storing and outputting results of the encrypting process and the MAC generating process; and

a selector for selecting alternately the results of the encrypting process and the MAC generating process from the memory to alternately

perform the encrypting process and the MAC generating process.

10. An encrypting method for encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the encrypting method comprising:

an encrypting step, including a first feedback step for feeding back ciphertext block data C_i output from the encrypting unit when the encrypting unit encrypts plaintext block data, inputting the plaintext block data, performing an encrypting process by feeding back the ciphertext block data C_i through a first feedback loop, and outputting a ciphertext block data; and

a MAC generating step, including a second feedback step for feeding back a computed intermediate MAC result, inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting step, processing data, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data.

11. A decrypting apparatus decrypting first processing data and second processing data comprising

a memory for storing a status of a decrypting process, and wherein

the decrypting apparatus starts the decrypting process of the second processing data before the decrypting process of the first processing data is completed,

the decrypting apparatus makes the memory store the status of the decrypting process of the first processing data when the decrypting process of the second processing data is started, and

the decrypting apparatus returns the status of the decrypting process of the decrypting apparatus to the status of the decrypting process of the first processing data stored in the memory when the decrypting process of the first processing data is restarted, and

the decrypting apparatus restarts the decrypting process of the first processing data.

12. The decrypting apparatus of claim 11, wherein

the decrypting apparatus restarts the decrypting process of the first processing data before the decrypting process of the second processing data is completed,

the memory stores the decrypting status of the second processing data when the decrypting process of the first processing data is restarted,

the decrypting apparatus returns the decrypting status of the decrypting apparatus to the decrypting status of the second processing data stored in the memory when the decrypting process of the second processing data is restarted, and

the decrypting apparatus restarts the decrypting process of the second processing data.

13. The decrypting apparatus of claim 11, wherein the first processing data is first ciphertext data, and the second processing data is second ciphertext data.

14. The decrypting apparatus of claim 11, wherein the decrypting apparatus starts the decrypting process of a first block data of the second processing data by an interrupt.

15. A decrypting apparatus decrypting ciphertext block data C_i (i = 1, 2, 3,

...) included in ciphertext data C and ciphertext block data D_j (j = 1, 2, 3, ...) included in ciphertext data D, the decrypting apparatus comprising:

a mechanism for receiving a request to decrypt the ciphertext data D at an arbitrary timing during a decrypting process of the ciphertext data C;

a decrypting unit for performing the decrypting process of the ciphertext block data C_i to output plaintext block data M_i;

a feedback loop for feeding back the ciphertext block data C_i to be used for decrypting ciphertext block data C_{i+1} to the decrypting unit through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving the request to decrypt the ciphertext data D and storing the ciphertext block data C_i fed back when the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i so that the decrypting process of any of ciphertext block data of the ciphertext data D is started; and

a selector for selecting and supplying the ciphertext block data C_i fed back from the feedback line of the feedback loop in case that the ciphertext block data C_{i+1} is decrypted subsequent to the ciphertext bock data C_i, and for selecting and supplying the ciphertext block data C_i stored in the memory in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i and the ciphertext block data C_{i+1} is decrypted after any of the ciphertext block data of the ciphertext data D is decrypted.

16. The decrypting apparatus of claim 15, wherein the memory includes:

plural registers corresponding to plural pieces of ciphertext data; and

a switch switching registers corresponding to the ciphertext data to

be decrypted.

17. A decrypting method comprising steps of:

decrypting ciphertext block data C_i (i = 1, 2, 3, ...) of first ciphertext data C using a decrypting module;

storing ciphertext block data C_i to be used for decrypting ciphertext block data C_{i+1} in a memory during or after decrypting the ciphertext block data C_i;

decrypting at least one ciphertext block data of a second ciphertext data D after storing the ciphertext block data C_i to be used for decrypting the ciphertext block data C_{i+1}; and

inputting the ciphertext block data C_i to be used for decrypting the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data of the ciphertext data D and decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module.

18. A decrypting apparatus decrypting ciphertext data including at least one ciphertext block data into plaintext data, and generating a message authentication code (MAC) for ensuring an integrity of ciphertext data, the decrypting apparatus comprising:

a decrypting unit, including a first feedback loop for feeding back module output block data T_i generated at decrypting data by a decrypting module, for inputting the ciphertext block data, decrypting the ciphertext block data using the module output block data T_i fed back through the first feedback loop, and outputting plaintext block data;

a MAC generator, including a second feedback loop for feeding back a

computed intermediate MAC result, for inputting ciphertext block data identical to the ciphertext block data input to the decrypting unit, processing the data, outputting the computed intermediate MAC result, feeding back the computed intermediate MAC result through the second feedback loop, and generating the MAC for ensuring the integrity of ciphertext data.

19. The decrypting apparatus of claim 18,

wherein the decrypting unit and the MAC generator share one decrypting module and one feedback loop and alternately perform a decrypting process and a MAC generating process, and

wherein the one feedback loop includes:

a memory storing and outputting results of the decrypting process and the MAC generating process; and

a selector for alternately selecting the results of the decrypting process and the MAC generating process to output to the decrypting module for alternately performing the decrypting process and the MAC generating process.

20. A decrypting method decrypting ciphertext data including at least one ciphertext block data into plaintext data and generating a message authentication code (MAC) for ensuring an integrity of the ciphertext data, the decrypting method comprising:

a decrypting step including a first feedback step for feeding back module output block data T_i generated at decrypting data by a decrypting module, inputting the ciphertext block data, decrypting the ciphertext block data using the module output block data T_i fed back through the first feedback loop, and outputting plaintext block data;

a MAC generating step including a second feedback step for feeding back a computed intermediate MAC result, inputting ciphertext block data identical to the ciphertext block data input to the decrypting unit, processing the data, outputting the computed intermediate MAC result, feeding back the computed intermediate MAC result by the second feedback loop, and generating the MAC for ensuring the integrity of ciphertext data.

21. An encrypting apparatus encrypting plaintext data M including plaintext block data M_i (i = 1, 2, 3, ...) and plaintext data N including plaintext block data N_j (j = 1, 2, 3, ...), the encrypting apparatus comprising:

a mechanism for receiving a request to encrypt the plaintext data N during encrypting process of the plaintext data M before completion of the encrypting process of the plaintext data M;

an encrypting module for outputting encrypted data as module output block data T_i;

a feedback loop for feeding back the module output block data T_i output from the encrypting module to the encrypting module through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving the request to encrypt the plaintext data N, and storing the module output block data T_i fed back when the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i so that an encrypting process of any plaintext block data of the plaintext data N is started; and

a selector for selecting and supplying the module output block data T_i fed back through the feedback line of the feed back loop to the feedback loop

in case that the plaintext block data M_{i+1} is encrypted subsequent to the plaintext block data M_i, and for selecting and supplying the module output block data T_i stored in the memory to the feedback loop in case that the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i and the plaintext block data M_{i+1} is encrypted after any of plaintext block data of the plaintext data N is encrypted.

22. The encrypting apparatus of claim 21, wherein the memory includes:

plural registers corresponding to plural pieces of plaintext data; and

a switch switching registers corresponding to the plaintext data to be encrypted.

23. An encrypting method comprising steps of:

encrypting plaintext block data M_i (i = 1, 2, 3, ...) of first plaintext data M using module output block data T_i (i = 1, 2, 3, ...) output from an encrypting module;

storing the module output block data T_i to be used for encrypting the plaintext block data M_{i+1} of the fist plaintext data M during or after encrypting the plaintext block data M_i;

encrypting at least one plaintext block data of second plaintext data N after storing the module output block data T_i to be used for encrypting the plaintext block data M_{i+1}; and

inputting the module output block data T_i to be used for encrypting the plaintext block data M_{i+1} stored in the memory after encrypting the at least one plaintext block data of the second plaintext data N and encrypting the plaintext block data M_i of the first plaintext data M using the encrypting module.

24. An encrypting apparatus encrypting plaintext data including at least one plaintext block data and generating a message authentication code (MAC) for ensuring an integrity of ciphertext data, the encrypting apparatus comprising:

an encrypting unit, having a first feedback loop for feeding back module output block data T_1 output from the encrypting module to the encrypting module when the plaintext block data is encrypted by the encrypting unit, for inputting the plaintext data, performing encrypting process by feeding back the module output block data T_1 through the first feedback loop, and outputting the ciphertext block data;

a MAC generator, having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting unit, processing data, feeding back the computed intermediate MAC result through the second feedback loop, and generating the MAC to ensure the integrity of the ciphertext data.

25. The encrypting apparatus of claim 24,

wherein the encrypting unit and the MAC generator share one encrypting module and one feedback loop to perform alternately the encrypting process and a MAC generating process, and

wherein the one feedback loop includes:

a memory for respectively storing and outputting results of the encrypting process and the MAC generating process; and

a selector for selecting alternately the results of the encrypting process and the MAC generating process from the memory to alternately

perform the encrypting process and the MAC generating process.

26. An encrypting method for encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data comprising:

an encrypting step, having a first feedback step for feeding back module output block data T_i output from an encrypting module when the plaintext block data is encrypted, for inputting the plaintext block data, performing an encrypting process by feeding back the module output block data T_i through a first feedback loop, and outputting ciphertext block data; and

a MAC generating step, having a second feedback step for feeding back a computed intermediate MAC result, for inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting step, processing data, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data.

27. A decrypting apparatus decrypting ciphertext data C including ciphertext block data C_i (i = 1, 2, 3, ...) and ciphertext data D including ciphertext block data D_j (j = 1, 2, 3, ...), the decrypting apparatus comprising:

a mechanism for receiving a request to decrypt the ciphertext data D during a decrypting process of the ciphertext data C;

a decrypting module for outputting decrypted data as module output block data T_i;

a feedback loop for feeding back the module output block data T_i

output from the decrypting module to the decrypting module through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving a request to decrypt the ciphertext data D and stores the module output block data T_i fed back in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i so that the decrypting process of any of the ciphertext block data of the ciphertext data D is started; and

a selector for selecting and supplying the module output block data T_i fed back through the feedback line of the feedback loop to the feedback loop in case that the ciphertext block data C_{i+1} is decrypted subsequent to the ciphertext block data C_i, and for selecting and supplying the module output block data T_i stored in the memory to supply to the feedback loop in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i and the ciphertext block data C_{i+1} is decrypted after any of the ciphertext block data of the ciphertext data D is decrypted.

28. The decrypting apparatus of claim 27, wherein the memory includes:

plural registers corresponding to plural ciphertext data; and

a switch for switching the plural registers corresponding to the ciphertext data to be decrypted.

29. A decrypting method comprising steps of:

decrypting ciphertext block data C_i (i = 1, 2, 3, ...) of first ciphertext data C using module output block data T_i (i = 1, 2, 3, ...) output from a decrypting module;

storing module output block data T_i to be used for decrypting

ciphertext block data C_{i+1} of the first ciphertext data C in a memory during or after a decrypting process of the ciphertext block data C_i;

decrypting at least one ciphertext block data of second ciphertext data D after storing the module output block data T_i to be used for decrypting the ciphertext block data C_{i+1} in the memory; and

decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module by inputting the module output block data T_i to be used for the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data of the second ciphertext data D.

30. A decrypting apparatus decrypting ciphertext data including at least one ciphertext block data into ciphertext data using a decrypting module and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the decrypting apparatus comprising:

a decrypting unit, having a first feedback loop for feeding back ciphertext block data C_i output from the decrypting unit to the decrypting unit when the ciphertext block data is decrypted by the decrypting unit, for inputting the ciphertext data, performing a decrypting process by feeding back the module output block data T_i through the first feedback loop, and outputting the ciphertext block data;

a message authentication code (MAC) generator having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data identical to the ciphertext block data input to the decrypting unit, processing data, feeding back the computed intermediate MAC result through the second feedback loop, and generating

the MAC to ensure the integrity of the ciphertext data.

31. The decrypting apparatus of claim 30,

wherein the decrypting unit and the MAC generator share one decrypting module and one feedback loop to perform alternately the decrypting process and a MAC generating process, and

wherein the one feedback loop includes:

a memory for respectively storing and outputting results of the decrypting process and the MAC generating process; and

a selector for selecting alternately the results of the decrypting process and the MAC generating process from the memory to alternately perform the decrypting process and the MAC generating process.

32. A decrypting method for decrypting ciphertext data including at least one ciphertext block data into plaintext data using a decrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the decrypting method comprising:

a decrypting step, having a first feedback step for feeding back ciphertext block data C_i, for inputting the ciphertext block data, performing a decrypting process of the ciphertext block data C_i fed back through the first feedback loop, and outputting plaintext block data; and

a MAC generating step, having a second feedback step for feeding back a computed intermediate MAC result, for inputting the ciphertext block data identical to the ciphertext block data input to the decrypting step, processing data to output the computed intermediate MAC result, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data.

33. A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 7.

34. A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 10.

35. A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 17.

36. A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 20.

37. A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 23.

38. A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 26.

39. A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 29.

40. A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 32.

41. The encrypting apparatus of claim 1, wherein the encrypting process is performed using block cipher algorithm.

42. The decrypting apparatus of claim 11, wherein the decrypting process is performed using block cipher algorithm.

43. The encrypting apparatus of claim 1, wherein the memory stores an intermediate encrypting result of the first processing data and an encryption key to be used for encrypting the first processing data as the status of the encrypting process.

44. The decrypting apparatus of claim 11, wherein the memory stores an

intermediate decrypting result of the second processing data and an encryption key to be used for decrypting the second processing data as the status of the decrypting process.

45. An encrypting apparatus comprising:

an encrypting unit for inputting data to encrypt and outputting encrypted data; and

a message authentication code (MAC) generator for inputting the encrypted data output from the encrypting unit and generating a MAC for ensuring an integrity of the encrypted data, and

wherein the MAC generator starts generating the MAC before completion of encrypting the data by the encrypting unit.

46. A decrypting apparatus comprising:

a decrypting unit for inputting data to decrypt and outputting decrypted data; and

a message authentication code (MAC) generator for inputting the decrypted data output from the decrypting unit and generating a MAC for ensuring an integrity of encrypted data, and

wherein the MAC generator starts generating the MAC before completion of decrypting the data by the decrypting unit.

47. An encrypting method comprising:

an encrypting step for inputting data to encrypt and outputting encrypted data; and

a MAC generating step for inputting the encrypted data output from the encrypting step and generating a MAC for ensuring an integrity of the encrypted data, and

wherein the MAC generating step starts generating the MAC before completion of encrypting the data by the encrypting step.

48. A decrypting method comprising:

a decrypting step for inputting data to decrypt and outputting decrypted data; and

a MAC generating step for inputting the decrypted data output from the decrypting step and generating a MAC for ensuring an integrity of the encrypted data, and

wherein the MAC generating step starts generating the MAC before completion of decrypting the data by the decrypting step.

49. A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 47.

50. A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 48.